

DESCRIPTION

PSEUDORANDOM NUMBER GENERATOR AND PSEUDORANDOM NUMBER GENERATION PROGRAM

Technical Field

[0001]

The present invention relates to a pseudorandom number generator and pseudorandom number generation program for generating pseudorandom numbers used for cryptocommunication.

Background Art

[0002]

Data communication through telephone, radio, the Internet, and the like is presently carried out by encrypting communication data to protect the data from wiretapping or alteration third persons. A sender of data encrypts the data with an encryption key and transmits the encrypted data. A receiver receives the encrypted data, decrypts the data with a decryption key, and obtains the data. Even if a third person intercepts the data, the third person has no authentic decryption key, and therefore, is unable to decrypt or tamper with the data.

[0003]

Cryptosystems include a common key cryptosystem and a public key cryptosystem. To best utilize the

characteristics of these systems, one of them must be selected according to conditions of use. Any system guarantees the security of communication data with the use of an encryption key, which is generated by using a pseudorandom number so that the encryption key may not easily be guessed.

[0004]

For example, a pseudorandom number generation method employing a linear feedback shift register is capable of generating a pseudorandom number sequence of long data length from a relatively short initial value for random number generation. This method allows a plurality of devices to generate the same pseudorandom numbers only by sharing an initial value. It is known that combining a plurality of linear feedback shift registers having primitive polynomials satisfying specific conditions as characteristic polynomials realizes a pseudorandom number generator that can generate unpredictable pseudorandom numbers. Without sharing an initial value, information for selecting a plurality of linear feedback shift registers may be shared to generate the same pseudorandom number sequence (for example, refer to Japanese Unexamined Patent Application Publication No. Hei-10-91066).

[0005]

The pseudorandom number generator employing linear feedback shift registers, however, generates pseudorandom numbers according to a specific algorism

even if it uses a combination of nonlinear operations. There is, therefore, a risk that pseudorandom numbers to be generated are guessed from an initial number or from part of a generated pseudorandom number sequence.

[0006]

If pseudorandom numbers are generated by selecting some of the plurality of linear feedback shift registers, it will be difficult to predict a pseudorandom number sequence to be generated. Combining linear feedback shift registers having characteristic polynomials of optional coefficients has a problem that it generates a pseudorandom number sequence that is not always an M-sequence (maximum length sequence) and the same pseudorandom number sequence is repeatedly generated at short intervals. It is necessary, therefore, to prepare many polynomials satisfying specific conditions in advance, select some from among them, and combine the selected ones. This means that linear feedback shift registers that are not always used must be arranged to deteriorate efficiency.

Disclosure of Invention

[0007]

An object of the present invention is to provide a pseudorandom number generator and pseudorandom number generation program appropriate for cryptocommunication and capable of generating a pseudorandom number sequence that is hardly predicted even if a generated pseudorandom

number sequence or transmitted/received data is observed.

[0008]

In order to accomplish the object, a first aspect of the present invention provides a pseudorandom number generator for generating a pseudorandom number sequence of a predetermined bit length, comprising a first linear feedback shift register having **m** steps of shift registers to provide a bit string of a predetermined bit length; a second linear feedback shift register having **n** steps of shift registers to provide a bit string of a predetermined bit length; an initial value generator to generate, according to predetermined conditions, initial values for the respective shift registers of the first linear feedback shift register and second linear feedback shift register and supply the initial values to the first linear feedback shift register and second linear feedback shift register; a polynomial coefficient generator to generate, according to predetermined conditions, coefficients of a characteristic polynomial of the second linear feedback shift register and supply the coefficients to the second linear feedback shift register; a primitive polynomial memory to store a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials serving as a characteristic polynomial of the first linear feedback shift register; a primitive polynomial

selector to select, according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory and supply coefficients of the primitive polynomial as coefficients of a characteristic polynomial to the first linear feedback shift register; and a pseudorandom number output unit to generate the pseudorandom number sequence of the predetermined bit length by carrying out bit-by-bit logical operations on the bit string provided by the first linear feedback shift register and the bit string provided by the second linear feedback shift register and output the pseudorandom number sequence.

[0009]

According to a second aspect of the present invention that is based on the first aspect, the pseudorandom number generator comprises a communication unit to generate initial data including the identification information of the primitive polynomial selected by the primitive polynomial selector, the initial values generated by the initial value generator for the shift registers of the first linear feedback shift register and second linear feedback shift register, and the coefficients of the characteristic polynomial generated by the polynomial coefficient generator, send the initial data to a second pseudorandom number generator, receive, if any, initial data from the second pseudorandom number generator, extract from the received initial data initial values for the first linear feedback

shift register and second linear feedback shift register, supply the extracted initial values to the first linear feedback shift register and second linear feedback shift register, extract coefficients for a characteristic polynomial from the received initial data, supply the extracted coefficients to the second linear feedback shift register, extract identification information of a primitive polynomial from the received initial data, and supply the extracted identification information to the primitive polynomial selector. The primitive polynomial selector selects one of the primitive polynomials stored in the primitive polynomial memory according to the identification information extracted by the communication unit and supplies coefficients of the primitive polynomial to the first linear feedback shift register.

[0010]

A third aspect of the present invention provides a pseudorandom number generation program executed by a computer to generate a pseudorandom number sequence of a predetermined bit length, the pseudorandom number generation program making the computer function as a first linear feedback shift register having **m** steps of shift registers to provide a bit string of a predetermined bit length; a second linear feedback shift register having **n** steps of shift registers to provide a bit string of a predetermined bit length; initial value generation means for generating, according to predetermined

conditions, initial values for the respective shift registers of the first linear feedback shift register and second linear feedback shift register and supplying the initial values to the first linear feedback shift register and second linear feedback shift register; polynomial coefficient generation means for generating, according to predetermined conditions, coefficients of a characteristic polynomial of the second linear feedback shift register and supplying the coefficients to the second linear feedback shift register; primitive polynomial memory means for storing a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials serving as a characteristic polynomial of the first linear feedback shift register; primitive polynomial selection means for selecting, according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory means and supplying coefficients of the primitive polynomial as coefficients of a characteristic polynomial to the first linear feedback shift register; and pseudorandom number output means for generating the pseudorandom number sequence of the predetermined bit length by carrying out bit-by-bit logical operations on the bit string provided by the first linear feedback shift register and the bit string provided by the second linear feedback shift register and outputting the pseudorandom number sequence.

[0011]

According to a fourth aspect of the present invention that is based on the third aspect, the pseudorandom number generation program further makes the computer function as communication means for generating initial data including the identification information of the primitive polynomial selected by the primitive polynomial selection means, the initial values generated by the initial value generation means for the shift registers of the first linear feedback shift register and second linear feedback shift register, and the coefficients of the characteristic polynomial generated by the polynomial coefficient generation means, sending the initial data to a second pseudorandom number generator, receiving, if any, initial data from the second pseudorandom number generator, extracting from the received initial data initial values for the first linear feedback shift register and second linear feedback shift register, supplying the extracted initial values to the first linear feedback shift register and second linear feedback shift register, extracting coefficients for a characteristic polynomial from the received initial data, supplying the extracted coefficients to the second linear feedback shift register, extracting identification information of a primitive polynomial from the received initial data, and supplying the extracted identification information to the primitive polynomial selection means; and the

primitive polynomial selection means selects one of the primitive polynomials stored in the primitive polynomial memory means according to the identification information extracted by the communication means and supplies coefficients of the primitive polynomial to the first linear feedback shift register.

Brief Description of Drawings

[0012]

[Fig.1] Figure 1 is a functional diagram showing a pseudorandom number generator according to a first embodiment.

[Fig.2] Figure 2 is a circuit diagram showing a first linear feedback shift register.

[Fig.3] Figure 3 is a circuit diagram showing a second linear feedback shift register.

[Fig.4] Figure 4 is a flowchart showing a pseudorandom generation process according to the first embodiment.

[Fig.5] Figure 5 is a view showing changes in values of the first and second linear feedback shift registers.

[Fig.6] Figure 6 is a functional diagram showing a pseudorandom number generator according to a second embodiment.

[Fig.7] Figure 7 is a flowchart showing a pseudorandom number generation process according to the second embodiment.

[Fig.8] Figure 8 is a functional diagram showing a pseudorandom number generator according to a third embodiment.

[Fig.9] Figure 9 is a flowchart showing a pseudorandom number generation process according to the third embodiment.

Best Mode for Carrying out the Invention

[0013]

Embodiments of the present invention will be explained with reference to Figs.1 to 9. The bit length of a pseudorandom number generated by a pseudorandom number generator 1 is h+1.

[0014]

<First embodiment>

In Fig.1, a pseudorandom number generator 1A according to the first embodiment has a first linear feedback shift register 2, a second linear feedback shift register 3, an initial value generator 4, a polynomial coefficient generator 5, and a pseudorandom number output unit 6.

[0015]

The first linear feedback shift register 2 is an m-step linear feedback shift register having **m** flip-flop circuits (to be explained later in detail). The second linear feedback shift register 3 is an n-step linear feedback shift register having **n** flip-flop circuits (to be explained later in detail).

[0016]

The initial value generator 4 has functions of using initial information to be provided externally or using predetermined conditions that may be obtained from always changing information such as date and time information or from physical phenomena such as heat, noise, and the like, generating initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) accordingly for the flip-flops of the first linear feedback shift register 2, supplying them to the first linear feedback shift register 2, generating initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) accordingly for the flip-flops of the second linear feedback shift register 3, and supplying them to the second linear feedback shift register 3. Not to make an output from the first linear feedback shift register 2 always "0," at least one of the initial values ia_{m-1} to ia_0 must be "1." Similarly, at least one of the initial values ib_{n-1} to ib_0 must be "1."

[0017]

The polynomial coefficient generator 5 has functions of using initial information to be provided externally or using predetermined conditions that may be obtained from always changing information such as date and time information or from physical phenomena such as heat, noise, and the like, generating coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) accordingly for a characteristic polynomial of the second linear feedback shift register 3, and supplying them to the

second linear feedback shift register 3.

[0018]

The pseudorandom number output unit 6 has functions of receiving a bit string **ra** (ra_0, ra_1, ..., ra_{h-1}, ra_h) sequentially provided by the first linear feedback shift register 2 and a bit string **rb** (rb_0, rb_1, ..., rb_{h-1}, rb_h) sequentially provided by the second linear feedback shift register 3, operating exclusive ORs of the respective bits, generating a pseudorandom number **r** (r_0, r_1, ..., r_{h-1}, r_h) of a predetermined bit length, and outputting the same.

[0019]

In Fig.2, the first linear feedback shift register 2 has the **m** flip-flop circuits, AND circuits, and XOR circuits. The characteristic polynomial of the first linear feedback shift register 2 is a predetermined primitive polynomial of $a_mX^m + a_{m-1}X^{m-1} + a_{m-2}X^{m-2} + \ldots + a_2X^2 + a_1X + a_0$ (where $a_m = 1$ and $a_0 = 1$). The coefficients **a** (a_{m-1}, ..., a_1) of the primitive polynomial are set to the AND circuits, respectively.

[0020]

If $a_i = 0$ ($0 < i < m$), the AND circuit provides "0" without regard to a value provided by the flip-flop FA_{i-1} ($0 < i < m$), and if $a_i = 1$ ($0 < i < m$), provides the value provided by the flip-flop FA_{i-1} ($0 < i < m$).

[0021]

In Fig.3, the second linear feedback shift register 3 has the **n** flip-flop circuits, AND circuits, and XOR

circuits. The characteristic polynomial of the second linear feedback shift register 3 may be $b_nX^n + b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \ldots + b_2X^2 + b_1X + b_0$. Then, the coefficients **b** (b_{n-1}, ..., b_1 = coefficients s) of the characteristic polynomial are set to the AND circuits, respectively.

[0022]

Accordingly, if $b_j = 0$ ($0 < j < n$), the AND circuit provides "0" without regard to a value provided by the flip-flop FB_{j-1} ($0 < j < n$), and if $b_j = 1$ ($0 < j < n$), provides the value provided by the flip-flop FB_{j-1} ($0 < j < n$).

[0023]

Next, operation of the pseudorandom number generator 1A will be explained with reference to the flowchart of Fig.4.

[0024]

When the pseudorandom number generator 1A starts a pseudorandom number generation process, the initial value generator 4 generates (step S01) initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) and initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) according to externally provided initial information or predetermined conditions and supplies the initial values to the first linear feedback shift register 2 and second linear feedback shift register 3.

[0025]

The polynomial coefficient generator 5 generates (step S02) coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) for

a characteristic polynomial of the second linear feedback shift register 3 according to externally provided initial information or predetermined conditions and supplies them to the second linear feedback shift register 3.

[0026]

Once the initial value generator 4 and polynomial coefficient generator 5 supply the initial values and coefficients, the first linear feedback shift register 2 and second linear feedback shift register 3 set (step S03) the initial values and coefficients to the flip-flop circuits and AND circuits and a value k = 0 to a counter **k** for counting the number of output bits. In the first linear feedback shift register 2, the initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) are set to the flip-flop circuits FA_{m-1}, FA_{m-2}, ..., FA_1, and FA_0, respectively, and the coefficients **a** (a_{m-1}, ..., a_1) of the primitive polynomial are set to the AND circuits, respectively. In the second linear feedback shift register 3, the initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) are set to the flip-flop circuits FB_{n-1}, FB_{n-2}, ..., FB_1, and FB_0, respectively, and the coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) of the characteristic polynomial are set to the AND circuits, respectively. In the second linear feedback shift register 3 of Fig.3, $b_n = 1$ and $b_0 = 1$. Instead, AND circuits may be provided for b_n and b_0 so that these coefficients may have optional values like the other coefficients.

[0027]

The first linear feedback shift register 2 receives (step S04) a clock signal, carries out an operation, and provides (step S05) a bit ra_k. Similarly, the second linear feedback shift register 3 receives (step S06) a clock signal, carries out an operation, and provides (step S07) a bit rb_k.

[0028]

The pseudorandom number output unit 6 receives the bit ra_k from the first linear feedback shift register 2 and the bit rb_k from the second linear feedback shift register 3, operates an exclusive OR of values of the bits, and generates (step S08) a bit r_k.

[0029]

Next, the first linear feedback shift register 2 and second linear feedback shift register 3 increment (step S09) the value of the counter **k** by one ($k \leftarrow k + 1$) and determine (step S10) whether or not the value of the counter **k** is higher than a value h. If the value of the counter **k** is equal to or less than **h**, the first linear feedback shift register 2 returns to step S04 and outputs a bit ra_{k+1}. Also, the second linear feedback shift register 3 returns to step S06 and outputs a bit rb_{k+1}. Then, the pseudorandom number output unit 6 generates a bit r_{k+1}.

[0030]

If the value of the counter **k** is larger than **h**, the pseudorandom number generator 1 ends the

pseudorandom number generation process and outputs (step S11) the generated bits r_0, r_1, ..., r_{h-1}, r_h as a pseudorandom number **r** (r_0, r_1, ..., r_{h-1}, r_h).

[0031]

This will be explained in detail with reference to Fig.5. As an example, an 8-bit pseudorandom number **r** is output. It is assumed that the primitive polynomial of the first linear feedback shift register 2 is $X^7 + X^3 + 1$, the first linear feedback shift register 2 has seven steps of flip-flop circuits and the initial values **ia** (ia_6, ia_5, ..., ia_1, ia_0) = (1, 0, 1, 0, 1, 0, 1), the second linear feedback shift register 3 has eight steps of flip-flop circuits and the initial values **ib** (ib_7, ib_6, ..., ib_1, ib_0) = (1, 1, 1, 1, 0, 0, 0, 0), and the characteristic polynomial of the second linear feedback shift register 3 has coefficients (s_7, s_6, ..., s_2, s_1) = (0, 1, 1, 1, 0, 1, 1).

[0032]

When a first clock signal is input, the first linear feedback shift register 2 shifts the bits as $FA_0 \rightarrow FA_1$, $FA_1 \rightarrow FA_2$, ..., $FA_5 \rightarrow FA_6$ to make (FA_6, FA_5, FA_4, FA_3, FA_2, FA_1) = (0, 1, 0, 1, 0, 1). The primitive polynomial of the first linear feedback shift register 2 is $X^7 + X^3 + 1$, and therefore, the bit "1" of FA_6 and the bit "1" shifted from FA_2 to FA_3 are exclusive-ORed (XORed) into "0" which is fed back to FA_0 to establish a state "+1" of Fig.5. As a result, the first linear feedback shift register 2 outputs "0" as ra_0.

[0033]

When the first clock signal is input, the second linear feedback shift register 3 shifts the bits as $FB_0 \rightarrow FB_1$, $FB_1 \rightarrow FB_2$, ..., $FB_6 \rightarrow FB_7$ to make (FB_7, FB_6, FB_5, FB_4, FB_3, FB_2, FB_1) = (1, 1, 1, 0, 0, 0, 0). The characteristic polynomial has the coefficients (s_7, s_6, ..., s_1, s_0) = (0, 1, 1, 1, 0, 1, 1), and therefore, the characteristic polynomial is $X^8 + X^6 + X^5 + X^4 + X^2 + X + 1$. The bit "1" shifted from FB_5 to FB_6, the bit "0" shifted from FB_3 to FB_4, the bit "0" shifted from FB_1 to FB_2, and the bit "0" shifted from FB_0 to FB_1 are XORed into "1" which is fed back to FB_0 to establish the state "+1" of Fig.5. As a result, the second linear feedback shift register 3 outputs "1" as rb_0.

[0034]

When a second clock signal is input, the first linear feedback shift register 2 and second linear feedback shift register 3 shift bits similarly, carry out feedback operations according to the primitive polynomial and characteristic polynomial, establish a state "+2" of Fig.5, and output $ra_1 = 0$ and $rb_1 = 1$, respectively.

[0035]

In this way, operations are repeated so that the first linear feedback shift register 2 outputs (ra_0, ra_1, ..., ra_6, ra_7) = (0, 0, 0, 0, 1, 0, 1, 1) and the second linear feedback shift register 3 outputs (rb_0, rb_1, ..., rb_6, rb_7) = (1, 1, 1, 1, 1, 0, 0, 1). (ra_0, ra_1, ..., ra_6, ra_7) = (0, 0, 0, 0, 1, 0, 1, 1) and (rb_0,

rb_1, ..., rb_6, rb_7) = (1, 1, 1, 1, 1, 0, 0, 1) are XORed to output a pseudorandom number r (r_0, r_1, ..., r_6, r_7) = (1, 1, 1, 1, 0, 0, 1, 0).

[0036]

<Second embodiment>

In Fig.6, a pseudorandom number generator 1B according to the second embodiment has a first linear feedback shift register 2, a second linear feedback shift register 3, an initial value generator 4, a polynomial coefficient generator 5, a pseudorandom number output unit 6, a primitive polynomial selector 7, and a primitive polynomial memory 8. The same parts as those of the first embodiment are represented with the same numerals and their detailed explanations are omitted.

[0037]

The primitive polynomial selector 7 has functions of referring to externally provided initial information, selecting one of primitive polynomials stored in the primitive polynomial memory 8 accordingly, and supplying coefficients **a** (a_{m-1}, ..., a_1) of the primitive polynomial serving as a characteristic polynomial to the first linear feedback shift register 2.

[0038]

The primitive polynomial memory 8 stores a plurality of primitive polynomials with identification information, for setting AND circuits of the first linear feedback shift register 2. The identification information is to specify a primitive polynomial and

may be a number, which will hereinafter be referred to as an identification number. The identification number can set the AND circuits with a smaller amount of information than the number of coefficients of a primitive polynomial. In Fig.6, the primitive polynomial memory 8 uses identification numbers each having a bit length of two to identify primitive polynomials, such as an identification number "00" for $X^7 + X^3 + 1$, an identification number "01" for $X^7 + X^3 + X^2 + X + 1$, an identification number "10" for $X^7 + X^4 + X^3 + X^2 + 1$, an identification number "11" for $X^7 + X^6 + X^5 + X^4 + X^2 + X + 1$, and the like.

[0039]

Operation of the pseudorandom number generator 1B will be explained with reference to a flowchart of Fig.7.

[0040]

When the pseudorandom number generator 1B starts a pseudorandom number generation process, the primitive polynomial selector 7 selects (step S21) one of the primitive polynomials of the primitive polynomial memory 8 according to externally provided initial information and supplies coefficients of the selected primitive polynomial as coefficients **a** (a_{m-1}, ..., a_1) of a characteristic polynomial to the first linear feedback shift register 2.

[0041]

The initial value generator 4 generates (step S22) initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) and initial

values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) according to externally provided initial information or predetermined conditions and supplies the initial values to the first linear feedback shift register 2 and second linear feedback shift register 3.

[0042]

The polynomial coefficient generator 5 generates (step S23) coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) for a characteristic polynomial of the second linear feedback shift register 3 according to externally provided initial information or predetermined conditions and supplies them to the second linear feedback shift register 3.

[0043]

Once the primitive polynomial selector 7, initial value generator 4, and polynomial coefficient generator 5 supply the initial values and coefficients, the first linear feedback shift register 2 and second linear feedback shift register 3 set (step S24) the initial values and coefficients to the flip-flop circuits and AND circuits and a value k = 0 to a counter **k** for counting the number of output bits. In the first linear feedback shift register 2, the initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) are set to the flip-flop circuits FA_{m-1}, FA_{m-2}, ..., FA_1, and FA_0, respectively, and the coefficients **a** (a_{m-1}, ..., a_1) of the characteristic polynomial supplied from the primitive polynomial selector 7 are set to the AND circuits, respectively. In the second linear

feedback shift register 3, the initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) are set to the flip-flop circuits FB_{n-1}, FB_{n-2}, ..., FB_1, and FB_0, respectively, and the coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) of the characteristic polynomial are set to the AND circuits, respectively. In the second linear feedback shift register 3 of Fig.3, $b_n = 1$ and $b_0 = 1$. Instead, AND circuits may be provided for b_n and b_0 so that these coefficients may have optional values like the other coefficients.

[0044]

Thereafter, the same operations as those of the first embodiment (step S04 to step S11) are carried out to output a pseudorandom number **r** (r_0, r_1, ..., r_{h-1}, r_h) (step S25 to step S32).

[0045]

<Third embodiment>

The third embodiment employs two pseudorandom number generators 1C. For example, one pseudorandom number generator 1 is arranged on a transmission side and the other pseudorandom number generator 1 is arranged on a receive side. The pseudorandom number generators 1C share characteristic polynomial coefficients and initial values (initial data), to generate the same pseudorandom number.

[0046]

In Fig.8, the pseudorandom number generator 1C according to the third embodiment has a first linear

feedback shift register 2, a second linear feedback shift register 3, an initial value generator 4, a polynomial coefficient generator 5, a pseudorandom number output unit 6, a primitive polynomial selector 7, a primitive polynomial memory 8, and a communication unit 9. The same parts as those of the first and second embodiments are represented with the same numerals and their detailed explanations are omitted. For the sake of convenience, each component of the pseudorandom number generator 1 on the initial data transmission side is suffixed with a letter "t" and each component of the pseudorandom number generator 1 on the initial data receive side is suffixed with a letter "r."

[0047]

The communication unit 9 has functions of referring to an identification number representative of a primitive polynomial selected by the primitive polynomial selector 7, initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) and initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) generated by the initial value generator 4, and coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) for a characteristic polynomial generated by the polynomial coefficient generator 5, generating initial data consisting of bit strings of the identification number of the primitive polynomial, the coefficients of the characteristic polynomial, and the initial values, and transmitting/receiving the initial data to/from the other pseudorandom number generator 1.

[0048]

The communication unit 9 also has functions of extracting, from the initial data, the initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) and coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) of the characteristic polynomial, supplying them to the second linear feedback shift register 3, extracting the initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) from the initial data, supplying them to the first linear feedback shift register 2, extracting the identification number of the primitive polynomial from the initial data, and supplying the same to the primitive polynomial selector 7.

[0049]

Operation of generating the same pseudorandom number from the two pseudorandom number generators 1C will be explained with reference to the flowchart of Fig.9.

[0050]

When the pseudorandom number generator 1Ct starts a pseudorandom number generation process, the primitive polynomial selector 7t selects (step S41) one of the primitive polynomials of the primitive polynomial memory 8t according to externally provided initial information and supplies coefficients of the selected primitive polynomial as coefficients **a** (a_{m-1}, ..., a_1) of a characteristic polynomial to the first linear feedback shift register 2t and an identification number representative of the primitive polynomial to the

communication unit 9t.

[0051]

The initial value generator 4t generates (step S42) initial values **ia** (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) and initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) according to externally provided initial information or predetermined conditions and supplies the initial values to the first linear feedback shift register 2t, second linear feedback shift register 3t, and communication unit 9t.

[0052]

The polynomial coefficient generator 5t generates (step S43) coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) for a characteristic polynomial of the second linear feedback shift register 3t according to externally provided initial information or predetermined conditions and supplies them to the second linear feedback shift register 3t and communication unit 9t.

[0053]

Once the primitive polynomial selector 7t, initial value generator 4t, and polynomial coefficient generator 5t supply the initial values and coefficients, the first linear feedback shift register 2t and second linear feedback shift register 3t set (step S44) the initial values and coefficients to flip-flop circuits and AND circuits and a value k = 0 to a counter **k** for counting the number of output bits. In the first linear feedback shift register 2t, the initial values **ia** (ia_{m-1}, ia_{m-2}, ...,

ia_1, ia_0) are set to the flip-flop circuits FA_{m-1}, FA_{m-2}, ..., FA_1, and FA_0, respectively, and the coefficients **a** (a_{m-1}, ..., a_1) of the characteristic polynomial supplied from the primitive polynomial selector 7t are set to the AND circuits, respectively. In the second linear feedback shift register 3t, the initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) are set to the flip-flop circuits FB_{n-1}, FB_{n-2}, ..., FB_1, and FB_0, respectively, and the coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) of the characteristic polynomial are set to the AND circuits, respectively. In the second linear feedback shift register 3 of Fig.3, $b_n = 1$ and $b_0 = 1$. Instead, AND circuits may be provided for b_n and b_0 so that these coefficients may have optional values like the other coefficients.

[0054]

The communication unit 9t generates initial data consisting of the bit values of the identification number representative of the primitive polynomial, the bit values of the coefficients of the characteristic polynomial, and the bit values of the initial values and transmits (step S45) the initial data to the pseudorandom number generator 1Cr. At this time, the communication unit 9t may encrypt the initial data according to a given cipher method and transmit the encrypted initial data.

[0055]

The identification number representative of the

primitive polynomial may consist of two bits ("10"), the initial value **ia** seven bits ("1010101"), the initial value **ib** eight bits ("11110000"), and the coefficient **s** for the characteristic polynomial seven bits ("0111011"). In this case, the initial data is a 24-bit data string (identification number | initial value **ia** | initial value **ib** | coefficient **s**) = (101010101111100000111011).

[0056]

Thereafter, the pseudorandom number generator 1Ct carries out the same operations as those of the first embodiment (step S04 to step S11) and outputs a pseudorandom number **r** (r_0, r_1, ..., r_{h-1}, r_h) (step S46 to step S51).

[0057]

On the other hand, the communication unit 9r of the pseudorandom number generator 1Cr receives (step S52) the initial data from the pseudorandom number generator 1Ct, extracts, from the received initial data, the initial values **ib** (ib_{n-1}, ib_{n-2}, ..., ib_1, ib_0) and coefficients **s** (s_{n-1}, s_{n-2}, ..., s_2, s_1) of the characteristic polynomial, supplies them to the second linear feedback register 3r, extracts the initial values ia (ia_{m-1}, ia_{m-2}, ..., ia_1, ia_0) from the initial data, supplies them to the first linear feedback shift register 2r, extracts the identification number of the primitive polynomial from the initial data, and supplies the same to the primitive polynomial selector 7r. If the received

initial data is encrypted, the communication unit 9 decrypts it into the initial data.

[0058]

When the identification number of the primitive polynomial is supplied, the primitive polynomial selector 7r selects (step S53) one primitive polynomial corresponding to the identification number from the primitive polynomial memory 8r and supplies coefficients of the selected primitive polynomial as coefficients **a** (a_{m-1}, ..., a_1) of a characteristic polynomial to the first linear feedback shift register 2r.

[0059]

Once the primitive polynomial selector 7r and communication unit 9r supply the initial values and coefficients, the first linear feedback shift register 2r and second linear feedback shift register 3r set (step S54) the initial values and coefficients to flip-flop circuits and AND circuits and a value k = 0 to a counter **k** for counting the number of output bits.

[0060]

Thereafter, the pseudorandom number generator 1Cr carries out the same operations as those of the first embodiment (step S04 to step S11) and outputs a pseudorandom number **r** (r_0, r_1, ..., r_{h-1}, r_h) (step S55 to step S60).

[0061]

In this way, the two pseudorandom number generators 1 share initial data and generate the same pseudorandom

number.

[0062]

The pseudorandom number generator 1 may be realized by making a general-purpose computer execute a pseudorandom number generation program describing the above-mentioned functions. The pseudorandom number generation program may be read from a storage medium and executed by a general-purpose computer, or may externally be transmitted through a network and executed by a general-purpose computer.

Industrial Applicability

[0063]

According to the present invention, a pseudorandom number sequence longer than a given M-sequence can always be generated, and not only initial values but also coefficients of a characteristic polynomial can optionally be set. Even if the generated pseudorandom number sequence is observed, it is difficult to predict a pseudorandom number sequence to be generated. Accordingly, the safety of a pseudorandom number sequence is secured and the safety of data to be communicated is guaranteed. If correspondence between identification information and a primitive polynomial is unknown, it is difficult to decrypt data to be communicated.

[0064]

A primitive polynomial set as a characteristic

polynomial of the first linear feedback shift register is selected with identification information whose data amount for transmission is smaller than that of coefficients of the polynomial. Namely, the identification information whose data amount is smaller than that of the primitive polynomial itself helps reduce an information amount.